REMARKS

Favorable reconsideration of this application in view of the remarks to follow is respectfully requested. Since the present Response raises no new issues, and in any event, places the application in better condition for consideration on appeal, entry of allowance thereof is respectfully requested under the provisions of 37 C.F.R. §1.116. Applicants have amended independent claims 1, 10 and 28 to better clarify the invention. Support for the amendments is found in the specification on page 4, paragraphs [0017 and 0019] and page 6, paragraph [0022]. Further search is not required for consideration of amended claims 1, 10 and 28 as the limitations added are components of the previously entered claims and therefore previous searches relating to current invention are applicable to amended claims 1, 10 and 28.

Claim Rejection – 35 U.S.C. §112, second paragraph

The Office Action rejected claims 1, 10, 21, and 28 as being indefinite for failing to particularly point out and distinctly claim the subject matter of the invention. Without conceding to the propriety of the rejection, claims 1, 10 and 28 are being amended to structure the claims with the use of a verb as suggested by the Examiner. Claim 21 is being canceled in this response. The subject matter of claim 21 is now included in claims 1, 10 and 28 and these claims are also being amended as suggested by the Examiner.

Claim Rejection – 35 U.S.C. §103(a)

The Office Action rejected claims 1, 3 - 6 under 35 U.S.C. §103(a) as allegedly being unpatentable over Anderson et al. (U.S. Patent Application No. 2002/0091824) in view of U.S. Patent No. 4,647,914 ("Alexander") and Lau (U.S. Patent Application No. 2002/0196147). Of

the pending claims, claim 1 is independent. In this reply, without conceding to the propriety of the rejections, applicant is amending independent claim to further clarify what is being claimed. Support for the amendment can be found on page 4, paragraph [0019] of the originally submitted specification. It states: "... Moreover, as discussed further below, the electronic devices may periodically communicate with the electronic devices server 105 to verify that they are installed in an authorized network."

According to Graham v. John Deere Co., 148 U.S.P.Q. 459 (Sup. Ct. 1966), a prima facie case of obviousness must include an evaluation of the differences between the scope and content of the prior art references and the claimed invention, and a determination of whether these differences would have been obvious to one of ordinary skill in the art.

Applicant's independent claim 1, as amended, recites an "electronic device in a local area network," comprising, *inter alia*, a control that causes the network interface to communicate a response to the security system via the connection point in response to receipt of the polling signal, said control generates an alarm if said electronic device is not present and, said control causes the network interface to communicate the response to the security system as an encrypted message using an encryption code that is unique to the electronic device; wherein said message includes an address and an identifier associated with the electronic device and said control verifies that said electronic device is installed in an authorized network based upon said address and said identifier; wherein said user interface is configured to allow a user to arm and disarm a building intrusion detection features separately from security features of said LAN.

In contrast, Anderson discloses a computer system called a "reporting and maintenance system" (RMS) that acts as an intermediary between devices of an enterprise and a central management facility. (Page 2, paragraph [0017] and FIG. 3, reference character numeral 300). In

other words, Anderson discloses the use of an SNMP protocol and features that come standard with enabling the use of such protocol. Simple Network Monitoring Protocol mainly communicates the status of network devices in messages called protocol data units (PDU). Such protocol would not be usable for causing the network interface to communicate the response to the security system as an encrypted message using an encryption code that is unique to the electronic device. The features embedded in the use of SNMP protocol would not allow for a message to be generated and then sent, and for such message to include an address and an identifier associated with the electronic device, and also the features of this protocol would not be able to provide enough data for any control function to verify that said electronic device is installed in an authorized network based upon said address and said identifier.

Moreover, no where in Anderson's disclosure does it disclose said control generates an alarm if said electronic device is not present and, said control causes the network interface to communicate the response to the security system as an encrypted message using an encryption code that is unique to the electronic device; wherein said message includes an address and an identifier associated with the electronic device and said control verifies that said electronic device is installed in an authorized network based upon said address and said identifier; wherein said user interface is configured to allow a user to arm and disarm a building intrusion detection features separately from security features of said LAN as recited in claim 1 of the present invention.

Neither Alexander nor Lau disclose such limitations. Because those references fail to disclose or suggest what Anderson lacks as explained above with respect to independent claim 1 as amended, this claim is believed to be unobvious over the cited references.

The Office Action rejected claim 8 under 35 U.S.C. §103(a) as allegedly being unpatentable over Anderson et al. (U.S. Patent Application No. 2002/0091824) in view of Nagel (U.S. Patent No. 7,181,017). Although claim 8 is being canceled in the present response, the subject matter of the claim is being included in independent claims 1, 10 and 28 as amended. The Examiner suggests that Anderson does not teach but Nagel teaches the "control causes the network to communicate the response to the security system as an encryption code that is unique to the electronic device". The applicants respectfully disagree as Nagel only teaches a particular method of encrypting and decrypting data using public encryption key system. (Nagel, column 26, lines 32 – 55). It is specifically provided in Nagel "The basic reason for public-key encryption system is to ensure both the security of the information transferred along a data line..." (Nagel, column 5, lines 27 – 29). This addition fails to disclose what Anderson lacks.

Moreover, no where in Anderson's disclosure does it disclose said control generates an alarm if said electronic device is not present and, said control causes the network interface to communicate the response to the security system as an encrypted message using an encryption code that is unique to the electronic device; wherein said message includes an address and an identifier associated with the electronic device and said control verifies that said electronic device is installed in an authorized network based upon said address and said identifier; wherein said user interface is configured to allow a user to arm and disarm a building intrusion detection features separately from security features of said LAN as recited in claim 1of the present invention.

Nagel does not disclose either of such limitations. Because those references fail to disclose or suggest what Anderson lacks as explained above with respect to addition of subject

matter of previously disclosed claim 8 to claims 1, 10 and 28 these claims as amended are believed to be unobvious over the cited references.

The Office Action rejected claims 7, 10, 12 – 17 under 35 U.S.C. §103(a) as allegedly being unpatentable over Anderson et al. (U.S. Patent Application No. 2002/0091824) in view of U.S. Patent No. 4,647,914 ("Alexander"), Lau (U.S. Patent Application No. 2002/0196147) and Davies (U.S. Patent Application No. 2004/0024869). Of the pending claims, claim 10 is independent. In this reply, without conceding to the propriety of the rejections, applicant is amending independent claim 10 to further clarify what is being claimed. Support for the amendment can be found on page 4, paragraph [0019] of the originally submitted specification.

According to Graham v. John Deere Co., 148 U.S.P.Q. 459 (Sup. Ct. 1966), a prima facie case of obviousness must include an evaluation of the differences between the scope and content of the prior art references and the claimed invention, and a determination of whether these differences would have been obvious to one of ordinary skill in the art.

Applicant's independent claim 10, as amended, recite an "electronic device in a local area network," comprising, *inter alia*, control that causes the network interface to communicate a response to the security system via the connection point in response to receipt of the polling signal, said control generates an alarm if said electronic device is not present and, said control causes the network interface to communicate the response to the security system as an encrypted message using an encryption code that is unique to the electronic device; wherein said message includes an address and an identifier associated with the electronic device and said control verifies that said electronic device is installed in an authorized network based upon said address and said identifier; wherein said user interface is configured to allow a user to arm and disarm a building intrusion detection features separately from security features of said LAN.

In contrast, Anderson discloses a computer system called a "reporting and maintenance system" (RMS) that acts as an intermediary between devices of an enterprise and a central management facility. (Page 2, paragraph [0017] and FIG. 3, reference character numeral 300). In other words, Anderson discloses the use of SNMP protocol, which communicates the status of network devices in messages called protocol data units (PDU). Such protocol would not be usable for causing the network interface to communicate the response to the security system as an encrypted message using an encryption code that is unique to the electronic device.

In addition, no where in Anderson's disclosure does it disclose said control generates an alarm if said electronic device is not present and, said control causes the network interface to communicate the response to the security system as an encrypted message using an encryption code that is unique to the electronic device; wherein said message includes an address and an identifier associated with the electronic device and said control verifies that said electronic device is installed in an authorized network based upon said address and said identifier; wherein said user interface is configured to allow a user to arm and disarm a building intrusion detection features separately from security features of said LAN as recited in claim 10 of the present invention.

Neither Alexander nor Lau, nor Davies disclose such limitations. Since those references fail to disclose or suggest what Anderson lacks as explained above with respect to independent claim 10 as amended, this claim is also believed to be unobvious over the cited references.

The Examiner further disagrees with the Applicant's arguments with respect to claims 1 and 10 as amended, in the later issued advisory action. More specifically, the Examiner interprets teachings of Lau in paragraphs [0044] – [0046] as generating an alarm if the device is not present. However, respectfully, applicants submit that this teaching is still short of describing

an electronic device in a local area network, comprising, *inter alia*, a control that causes the network interface to communicate a response to the security system via the connection point in response to receipt of the polling signal, *said control verifies that said electronic device is installed in an authorized network* and generates an alarm if said electronic device is not present.

In response to the Applicant's argument referring to Anderson's disclosure of the use of an SNMP protocol, which would not be usable to cause the network interface to communicate the response to the security system as a message with address and identifier, the Examiner submitted that Anderson in paragraphs [0073] and [0074] teaches alternative protocols commonly used for status poling of multiple devices. Respectfully, it is applicant's position that such "status polling" is not what is being claimed. The functionality of network interfaces to communicate more detailed device information with address, location and other identifiers, as recited in claims 1 and 10, as amended, will not be possible with the use of SNMP *or like protocols* as suggested by Anderson.

The Office Action rejected claims 21 – 24, 26, 28 - 33 under 35 U.S.C. §103(a) as allegedly being unpatentable over Nagel (U.S. Patent No. 7,181,017) in view of U.S. Patent No. 4,647,914 ("Alexander") and Lau (U.S. Patent Application No. 2002/0196147). Of the pending claims, claims 21 and 28 are independent. In this reply, without conceding to the propriety of the rejections, applicant is canceling claim 21 and including its subject matter into independent claims 1, 10 and 28; and amending independent claim 28 to further clarify what is being claimed. Support for these amendments can be found on page 4, paragraph [0019] of the originally submitted specification.

According to Graham v. John Deere Co., 148 U.S.P.Q. 459 (Sup. Ct. 1966), a prima facie case of obviousness must include an evaluation of the differences between the scope and content

of the prior art references and the claimed invention, and a determination of whether these differences would have been obvious to one of ordinary skill in the art.

Applicant's independent claim 28, as amended, recites an "A security system server" comprising, *inter alia*, control means for determining whether the address is consistent with the identifier, said control means verifies that said electronic device is installed in an authorized network based upon said address and said identifier and generates an alarm if said electronic device is not present, and said control causes the network interface to communicate the response to the security system as an encrypted message using an encryption code that is unique to the electronic device; wherein said message includes an address and an identifier associated with the electronic device; and said network interface is configured to allow a user to arm and disarm a building intrusion detection features separately from security features of said LAN.

In contrast, Nagel discloses a system for obscuring at least a portion of the information communicated between systems on a network, communicating the encrypted information to a party, and decrypting the encrypted information using the negotiated comprehension function. In other words Nagel teaches a system for securing communication over networks. No where does it disclose control means for determining whether the address is consistent with the identifier, said control means verifies that said electronic device is installed in an authorized network based upon said address and said identifier and generates an alarm if said electronic device is not present, and said control causes the network interface to communicate the response to the security system as an encrypted message using an encryption code that is unique to the electronic device; wherein said message includes an address and an identifier associated with the electronic device; and said network interface is configured to allow a user to arm and disarm a building

intrusion detection features separately from security features of said LAN as recited in claim 28 of the present invention.

Neither Alexander nor Lau disclose such limitations. Because those references fail to disclose or suggest what Anderson lacks as explained above with respect to independent claim 28 as amended, this claim is also believed to be unobvious over the cited references. Applicant respectfully requests withdrawal of this ground of rejection.

The subjected matter of previously disclosed claim 21 is now incorporated in independent claims 1, 10 and 28 and it recites an electronic device comprising, *inter alia*, a control that causes the network interface to transmit a message, wherein said message includes an address and an identifier associated with the electronic device and said control verifies that said electronic device is installed in an authorized network based upon said address and said identifier. In contrast, Nagel discloses a system for obscuring at least a portion of the information communicated between systems on a network, communicating the encrypted information to a party, and decrypting the encrypted information using the negotiated comprehension function. In other words Nagel teaches a system for securing communication over networks.

Neither Alexander nor Lau disclose such limitations. Because those references fail to disclose or suggest what Anderson lacks as explained above with respect to the subject matter of previously disclosed claim 21, whose subject matter is now included in independent claims 1, 10 and 28 as amended, these claim is also believed to be unobvious over the cited references. Applicant respectfully requests withdrawal of this ground of rejection.

With regards to the rejections of the dependent claims in the instant Office Action, Applicant contents that dependent claims 2-9, 11-20, 22-27 and 29-34 are dependent from base claims 1, 10 and 28, and at least by virtue of their dependency are not obvious over cited

reference. Respectively they are now believed patentable due to the above-mentioned amendments to the base claims. Applicant respectfully requests withdrawal of these grounds of rejection.

In view of the foregoing, Applicant respectfully requests reconsideration, withdrawal of all rejections, and allowance of all pending claims in due course.

If the Examiner should have any questions concerning this communication or feels that an interview would be helpful, the Examiner is requested to call Applicant's undersigned attorney at the number indicated below.

Respectfully submitted,

Paul J. Esatto, Jr.
Registration No. 30,749

SCULLY, SCOTT, MURPHY & PRESSER, P.C.
400 Garden City Plaza - Suite 300
Garden City, New York 11530
(516) 742-4343

PJE:GS:me